UNIVERSITY OF CAMBRIDGE

General Data Protection Regulation: Changes and Implementation

James Knapton, Information Compliance Officer, Registrary's Office

Contents

- What is the GDPR?
- Key changes from the Data Protection Act 1998
- How the University is managing its preparations

What is the GDPR?

- EU General Data Protection Regulation applies *in full* from 25 May 2018
- Data Protection Act 1998 repealed on same date
- Will apply in UK despite and beyond Brexit
- Sets standards for handling ('processing') of information ('personal data') about living identifiable individuals ('data subjects') by organisations ('data controllers')
  - ➢ Uses existing concepts of data protection principles and data subject rights
  - ➢ Certain types of activity exempt from certain aspects of the standards
- More prescriptive and punitive than DPA: Information Commissioner's Office (ICO) fines up to €20m instead of £500k
- Supplemented by new UK Data Protection Bill (published September 2017 to apply by May 2018) that adds additional rules and exemptions

Key changes from DPA: Principles

DPA	GDPR
Personal data shall be:	**Personal data shall be:**
Processed fairly and lawfully	Processed fairly, lawfully and transparently
Processed only for specified and lawful purposes	Processed only for specified, explicit and legitimate purposes
Adequate, relevant and not excessive	Adequate, relevant and limited
Accurate	Accurate and rectified if inaccurate
Not kept for longer than necessary	Not kept for longer than necessary
Processed in accordance with data subjects' rights	Not a principle but covered elsewhere in GDPR
Processed securely	Processed securely
Not transferred outside the EEA without adequate protection	Not a principle but covered elsewhere in GDPR
Not covered in DPA	Data controller must be able to demonstrate compliance with principles

Key changes from DPA: Lawfulness (1)

- Under DPA, need to meet a ‘condition for processing’ for personal data use
  - With consent
  - To operate a contract
  - To meet a legal obligation
  - To protect the data subject’s vital interests
  - To perform a public interest task
  - To further the legitimate interests of the data controller
- Under GDPR, these are reformulated as ‘legal bases for processing’
  - Higher standard of consent – freely given, specific, informed, demonstrable
  - ‘Legitimate interests’ invalid for public authorities ‘in the performance of their tasks’

Key changes from DPA: Lawfulness (2)

- For ‘special category personal data’ (more sensitive information), need an additional legal basis
  - With explicit consent
  - To make/defend legal claims or prevent/detect crime
  - For medical purposes
  - For research purposes
  - And more…
- University needs to:
  - Reconsider its legal basis for each type of data use for each type of data subject (applicants, students, alumni, staff, research participants…)
  - Realign its engagement mechanisms with different types of data subject

Key changes from DPA: Privacy notices

- DPA: need to tell individuals
  - Who you are
  - How you'll use their data
- GDPR: need to do this plus
  - Must cover numerous extra topics, including the legal basis relied upon, retention periods, data sharing, the existence of data subject rights…
  - Must be transparently worded and accessible
- All University privacy notices need to be rewritten and (where possible) rationalised and standardised

Key changes from DPA: Rights

- Enhanced rights of:
  - Access
  - Rectification of inaccurate personal data
  - Restriction pending verification or correction
  - Objection (including to profiling and direct marketing)
- New rights of:
  - Erasure (‘the right to be forgotten’)
  - Portability
- All rights are qualified, and UK’s DP Bill adds numerous specific exemptions
- University needs to assess its systems and processes to enable the rights to be fulfilled if exercised

Key changes from DPA: Accountability

- New focus in GDPR on accountability measures
  - Policies and procedures to promote data protection by design and default, including Data Protection Impact Assessments for ‘high risk’ processing
  - Detailed rules surrounding contracts with joint data controllers and with data processors
  - Maintenance of a personal data register
  - Newly prescriptive requirements about security, including reporting certain personal data breaches to ICO within 72 hours
  - Newly prescribed role of Data Protection Officer
- All require new / revised policies, guidance, records, training, ways of working…

Key changes from DPA: Specific research exemptions

- Member States can vary rules for data processing for specific activities
- Research exemptions under GDPR and UK's DP Bill
  - Processing for journalism, art and 'academic purposes' exempt from all principles, legal bases, privacy notices and rights
  - Processing for archiving, statistics and 'scientific or historical research purposes' exempt from some principles and some rights, but not legal bases or privacy notices
  - Accountability requirements still apply

How the University is managing its preparations

- GDPR Data Protection Working Group established summer 2016
- Chaired by Registrary
- Members from Registrary's Office, LSO, Student Registry, CAO, ESP, UIS, CUDAR, Research Office, HR, UL, OIS, academic departments, CA, CUP
- Terms of Reference: "To develop, scrutinise and approve the necessary changes to the University's policies, procedures, guidelines and training in time for the implementation of the EU's General Data Protection Regulation. Where formal Committee oversight is required for any particular change, to develop, scrutinise and recommend the necessary change to the relevant Committee."
- Many changes can be implemented centrally
- GDPR Toolkit for Institutions for changes that must be implemented locally

Further information

- Website (Raven required)

  https://www.information-compliance.admin.cam.ac.uk/data-protection/general-data-protection-regulation

- Email

  data.protection@admin.cam.ac.uk